Project 2: Shift Register Sequences

Group 06: Fredrick Nilsson

November 29, 2023

Contents

Home Exercise 1

..

1. $p(x) = x^4 + x^2 + 1$ over $\mathbb{F}_2$

Since $x^4 + x^2 + 1 = (x^2 + x + 1)^2$ it is not irreducible, and therefore not primitive.

2. $p(x) = x^3 + x + 1$ over $\mathbb{F}_3$

Since $x^3 + x + 1 = x^3 + 3x^2 + 4x + 4 = (x + 2)(x^2 + x + 2)$, it clearly has factors and is therefore not irreducible. Since it is not irreducible, it is not primitive.

3. $p(x) = x^2 + \alpha^5 x + 1$ over $\mathbb{F}_{2^4}$, where $\alpha^4 + \alpha + 1 = 0$

If there is an i such that $p(a^i) = 0$, then $p(x)$ has a root, and is therefore not primitive nor irreducible.
If $i = 6$, then $p(\alpha^6) = \alpha^{12} + \alpha^{11} + 1 = (\alpha^3 + \alpha^2 + \alpha + 1) + (\alpha^3 + \alpha^2 + \alpha) + 1 = 2\alpha^3 + 2\alpha^2 + 2\alpha + 2 = 0$ As shown, $p(x)$ is reducible and therefore not primitive.

Lab Exercise 1

1. $p(x) = x^{23} + x^5 + 1$ over $\mathbb{F}_2$

```
> Primitive(x^23 + x^5 + 1) mod 2
> True
```

Therefore $p(x)$ is primitive, and therefore irreducible.

2. $p(x) = x^{23} + x^6 + 1$ over $\mathbb{F}_2$

```
> Primitive(x^23 + x^6 + 1) mod 2
> False
> Irreduc(x^23 + x^6 + 1) mod 2
> False
```

Therefore $p(x)$ is neither a primitive nor irreducible.

3. $p(x) = x^{18} + x^3 + 1$ over $\mathbb{F}_2$

```
> Primitive($x^{18} + x^3 + 1$) mod 2
> False
> Irreduc($x^{18} + x^3 + 1$) mod 2
> True
```

Therefore $p(x)$ is not a primitive, but it is irreducible.

4. $p(x) = x^8 + x^6 + 1$ over $\mathbb{F}_7$

```
> Primitive($x^8 + x^6 + 1$) mod 7
> False
> Irreduc($x^8 + x^6 + 1$) mod 7
> False
```

Therefore $p(x)$ is neither a primitive nor irreducible.

5. $p(x) = x^6 + \alpha^5 x + 1$ over $\mathbb{F}_{2^4}$

```
> Primitive($x^{23} + x^6 + 1$) mod 2
> True
```

Therefore $p(x)$ is primitive.

Home Exercise 2

$|\mathbb{F}_{2^4}| = 16 \implies \alpha^{15} \equiv 1$, therefore the possible orders for a polynomial consisting of one α are all possible factors of 15, that is 1, 3, 5 and 15.

1. α

$ord(\alpha) = n \implies \alpha^n \equiv \alpha^{15} \implies n = 15.$ The order of α is 15.

2. α^2

$ord(\alpha) = n \implies \alpha^{2n} \equiv \alpha^{15} \implies n = 15.$ The order of α is 15.

3. α^3

$ord(\alpha) = n \implies \alpha^{3n} \equiv \alpha^{15} \implies n = 5.$ The order of α is 5.

4. α^5

$ord(\alpha) = n \implies \alpha^{5^n} \equiv \alpha^{15} \implies n = 3$. The order of α is 3.

Lab Exercise 2

```
> G18 := GF(2, 18, $\alpha^{18}$ + $\alpha^3$ + 1)
> G18 := $\mathbb{F}_{2^{18}}$
```

1. α

```
> a := G18:-ConvertIn($\alpha$);
> ...
> G18:-order(a)
> 189
```

2. α^2

```
> a := G18:-ConvertIn($\alpha^2$);
> ...
> G18:-order(a)
> 189
```

3. α^3

```
> a := G18:-ConvertIn($\alpha^3$);
> ...
> G18:-order(a)
> 63
```

4. $\alpha + \alpha^3$

```
> a := G18:-ConvertIn($\alpha + \alpha^3$);
> ...
> G18:-order(a)
> 262143
```

Home Exercise 3

Lab Exercise 3

Home Exercise 4

Lab Exercise 4

Home Exercise 5

Lab Exercise 5

asdaadsssd[1]

References

[1] Wikipedia. Shift register. https://en.wikipedia.org/wiki/Shift_register, 2023. [Online; accessed 24-November-2023].